STORZ
KARL STORZ—ENDOSKOPE

ENDOSCOPES FOR MEDICINE AND TECHNICAL SCIENCE
INSTRUMENTS FOR OTO-RHINO-LARYNGOLOGY

January 15, 2020 Security Notice CVE-2020-0601

To whom it may concern,

Microsoft (CVE-2020-0601) Windows CryptoAPI Spoofing Vulnerability

Dear Sir or Madam,

KARL STORZ is aware of and currently monitoring the Windows CryptoAPI Vulnerability (CVE-2020-0601). This vulnerability was announced by Microsoft on January 14, 2020. This vulnerability affects Windows 10, Windows Server 2016, and Windows 2019 Server systems.

A spoofing vulnerability exists in the way Windows CryptoAPI (Crypt32.dll) validates Elliptic Curve Cryptography (ECC) certificates. An attacker could exploit the vulnerability by using a spoofed code-signing certificate to sign a malicious executable, making it appear the file was from a trusted, legitimate source. The user would have no way of knowing the file was malicious, because the digital signature would appear to be from a trusted provider. A successful exploit could also allow the attacker to conduct man-in-the-middle attacks and decrypt confidential information on user connections to the affected software.

KARL STORZ has had no reports of this vulnerability being exploited on a KARL STORZ product, but is currently working to test and validate the Microsoft patch for KARL STORZ products. A KARL STORZ Security Patch release will be made available to customers. Currently, Microsoft has not identified any mitigating factors or workarounds for this vulnerability.

Mitigation

- Microsoft has not identified any mitigating factors for this vulnerability.

Workaround

- Microsoft has not identified any workarounds for this vulnerability.

Employ Good Network Hygiene Practices

- Ensure data has been backed up and stored according to your individual processes and disaster recovery procedures
- Execute updates to malware protection, where available

Customers that maintain Virtual Machine (VM) system patches independent of KARL STORZ patch release should ensure these actions are performed to maintain the correct security posture of the system(s).

- For more information and instructions on how to apply the Microsoft security patch, please follow the link below:
  - https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2020-0601#ID0EA

KARL STORZ will provide a follow-up communication upon completion of our testing and verification of the Microsoft patch on any effected systems. If you have questions please contact us using the contact address: robert.haack@karlstorz.com.